Symantec™ Storage Foundation and High Availability Solutions 6.2 Readme First - Solaris

Installing Symantec Storage Foundation and High Availability Solutions products

This document includes the following topics:

- Installing and upgrading prerequisites

- About the script-based installer

- About the web-based installer

- Starting and stopping processes for the Symantec products

- Restarting the installer after a failed connection

- Installation program has improved failure handling

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Important release information

- For important updates regarding this release, review the Late-Breaking News TechNote on the Symantec Technical Support website:
  http://www.symantec.com/docs/TECH225259

- For the latest patches available for this release, go to:
  https://sort.symantec.com/

- The hardware compatibility list contains information about supported hardware and is updated regularly. For the latest information on supported hardware, visit the following URL:
  http://www.symantec.com/docs/TECH211575

- The software compatibility list summarizes each Storage Foundation and High Availability (SFHA) Solutions product stack and the product features, operating system versions, and third-party products it supports. For the latest information on supported software, visit the following URL:
  http://www.symantec.com/docs/TECH225258

Note: Before you install or upgrade SFHA Solutions products, review the current compatibility lists to confirm the compatibility of your hardware and software.

About Symantec Operations Readiness Tools

Symantec Operations Readiness Tools (SORT) is a website that automates and simplifies some of the most time-consuming administrative tasks. SORT helps you manage your datacenter more efficiently and get the most out of your Symantec products.

SORT can help you do the following:

Prepare for your next installation or upgrade	■ List product installation and upgrade requirements, including operating system versions, memory, disk space, and architecture. ■ Analyze systems to determine if they are ready to install or upgrade Symantec products and generate an Installation and Upgrade custom report. ■ List patches by product or platform, and in the order they need to be installed. Display and download the most recent patches or historical patches. ■ Display Array Support Library (ASL) details by vendor, platform, or Storage Foundation and High Availability (SFHA) version. ASLs make it easier to manage arrays that are connected to SFHA-based servers. ■ List VCS and ApplicationHA agents, documentation, and downloads based on the agent type, application, and platform.
Identify risks and get server-specific recommendations	■ Analyze your servers for potential environmental risks. Generate a Risk Assessment custom report with specific recommendations about system availability, storage use, performance, and best practices. ■ Display descriptions and solutions for thousands of Symantec error codes.
Improve efficiency	■ Get automatic email notifications about changes to patches, array-specific modules (ASLs/APMs/DDIs/DDLs), documentation, product releases, Hardware Compatibility Lists (HCLs), and VCS/ApplicationHA agents. ■ Quickly gather installed Symantec product and license key information from across your production environment. Generate a License/Deployment custom report that includes product names, versions, and platforms, server tiers, Symantec Performance Value Units (SPVUs), and End of Service Life dates. ■ List and download Symantec product documentation including product guides, manual pages, compatibility lists, and support articles. ■ Access links to important resources on a single page, including Symantec product support, SymConnect forums, customer care, Symantec training and education, Symantec FileConnect, the licensing portal, and my.symantec.com. The page also includes links to key vendor support sites. ■ Use a subset of SORT features from your iOS device. Download the application at: https://sort.symantec.com/mobile

> **Note:** Certain features of SORT are not available for all products. Access to SORT is available at no extra cost.

To access SORT, go to:

https://sort.symantec.com

System requirements

See your product Release Notes for more information.

Performing preinstallation checks and configuration

This document is designed for system administrators who already have a knowledge of basic UNIX system and network administration. Basic knowledge includes commands such as `tar`, `mkdir`, and simple shell scripting. Also required is basic familiarity with the specific platform and operating system where the Symantec product is installed.

Only users with superuser (`root`) privileges can install Symantec products.

Review the preinstallation requirements and system requirements. Install the operating system before installing the Symantec software.

Mount the Symantec software disc, or download and uncompress the Symantec software.

If patches to the Solaris operating system are required, the patches should be applied prior to installing the Symantec products. Patches may be required to resolve Solaris kernel, product performance, or other issues.

See the product *Release Notes* for last minute information on recommended patches.

For remote installation, or installation on multiple systems, set up rsh or ssh.

See "About configuring secure shell or remote shell communication modes before installing products" on page 7.

Prechecking your systems using the installer

The script-based and web-based installer's precheck option checks for the following:

- Recommended swap space for installation

- Recommended memory sizes on target systems for Symantec programs for best performance

- Required operating system versions

To use the precheck option

1   Start the script-based or web-based installer.

2   Select the precheck option:

- From the web-based installer, select the **Perform a Pre-Installation Check** from the Task pull-down menu.

- In the script-based installer, from root on the system where you want to perform the check, start the installer.

  ```
  # ./installer
  ```

  In the Task Menu, press the p key to start the precheck.

3   Enter the system name or the IP address of the system that you want to check.

4   Review the output and make the changes that the installer recommends.

About configuring secure shell or remote shell communication modes before installing products

Establishing communication between nodes is required to install Symantec software from a remote system, or to install and configure a cluster. The node from which the installer is run must have permissions to run `rsh` (remote shell) or `ssh` (secure shell) utilities. You need to run the installer with superuser privileges on the systems where you plan to install Symantec software.

You can install products to remote systems using either secure shell (ssh) or remote shell (rsh). Symantec recommends that you use ssh as it is more secure than rsh.

You can set up ssh and rsh connections in many ways.

- You can manually set up the SSH and RSH connection with UNIX shell commands.

- You can run the `installer -comsetup` command to interactively set up SSH and RSH connection.

- You can run the password utility, `pwdutil.pl`.

This section contains an example of how to set up ssh password free communication. The example sets up ssh between a source system (sys1) that contains the installation directories, and a target system (sys2). This procedure also applies to multiple target systems.

Note: The script- and web-based installers support establishing passwordless communication for you.

Manually configuring passwordless ssh

The ssh program enables you to log into and execute commands on a remote system. ssh enables encrypted communications and an authentication process between two untrusted hosts over an insecure network.

In this procedure, you first create a DSA key pair. From the key pair, you append the public key from the source system to the authorized_keys file on the target systems.

Read the ssh documentation and online manual pages before enabling ssh. Contact your operating system support provider for issues regarding ssh configuration.

Visit the OpenSSH website that is located at: http://openssh.org to access online manuals and other resources.

To create the DSA key pair

1   On the source system (sys1), log in as root, and navigate to the root directory.

```
sys1 # cd /
```

2   Make sure the /.ssh directory is on all the target installation systems (sys2 in this example). If that directory is not present, create it on all the target systems and set the write permission to root only:

Solaris 10:

```
sys2 # mkdir /.ssh
```

Solaris 11:

```
sys2 # mkdir /root/.ssh
```

Change the permissions of this directory, to secure it.

Solaris 10:

```
sys2 # chmod go-w /.ssh
```

Solaris 11:

```
sys2 # chmod go-w /root/.ssh
```

3 To generate a DSA key pair on the source system, type the following command:

```
sys1 # ssh-keygen -t dsa
```

System output similar to the following is displayed:

```
Generating public/private dsa key pair.
Enter file in which to save the key (//.ssh/id_dsa):
```

For Solaris 11:

```
Your identification has been saved in /root/.ssh/id_dsa.
Your public key has been saved in /root/.ssh/id_dsa.pub.
```

4 Press Enter to accept the default location of `/.ssh/id_dsa`.

5 When the program asks you to enter the passphrase, press the Enter key twice.

```
Enter passphrase (empty for no passphrase):
```

Do not enter a passphrase. Press Enter.

```
Enter same passphrase again:
```

Press Enter again.

To append the public key from the source system to the authorized_keys file on the target system, using secure file transfer

1 Make sure the secure file transfer program (SFTP) is enabled on all the target installation systems (sys2 in this example).

To enable SFTP, the `/etc/ssh/sshd_config` file must contain the following two lines:

```
PermitRootLogin          yes
  Subsystem          sftp      /usr/lib/ssh/sftp-server
```

2 If the lines are not there, add them and restart ssh.

To restart ssh on Solaris 10 and Solaris 11, type the following command:

```
sys1 # svcadm restart ssh
```

3   From the source system (sys1), move the public key to a temporary file on the target system (sys2).

Use the secure file transfer program.

In this example, the file name `id_dsa.pub` in the root directory is the name for the temporary file for the public key.

Use the following command for secure file transfer:

```
sys1 # sftp sys2
```

If the secure file transfer is set up for the first time on this system, output similar to the following lines is displayed:

```
Connecting to sys2 ...
The authenticity of host 'sys2 (10.182.00.00)'
can't be established. DSA key fingerprint is
fb:6f:9f:61:91:9d:44:6b:87:86:ef:68:a6:fd:88:7d.
Are you sure you want to continue connecting (yes/no)?
```

4   Enter `yes`.

Output similar to the following is displayed:

```
Warning: Permanently added 'sys2,10.182.00.00'
(DSA) to the list of known hosts.
root@sys2 password:
```

5   Enter the root password of sys2.

6   At the `sftp` prompt, type the following command:

```
sftp> put /.ssh/id_dsa.pub
```

The following output is displayed:

```
Uploading /.ssh/id_dsa.pub to /id_dsa.pub
```

7   To quit the SFTP session, type the following command:

```
sftp> quit
```

8 To begin the `ssh` session on the target system (sys2 in this example), type the following command on sys1:

```
sys1 # ssh sys2
```

Enter the root password of sys2 at the prompt:

```
password:
```

9 After you log in to sys2, enter the following command to append the `id_dsa.pub` file to the `authorized_keys` file:

```
sys2 # cat /id_dsa.pub >> /.ssh/authorized_keys
```

10 After the `id_dsa.pub` public key file is copied to the target system (sys2), and added to the authorized keys file, delete it. To delete the `id_dsa.pub` public key file, enter the following command on sys2:

```
sys2 # rm /id_dsa.pub
```

11 To log out of the `ssh` session, enter the following command:

```
sys2 # exit
```

12 Run the following commands on the source installation system. If your ssh session has expired or terminated, you can also run these commands to renew the session. These commands bring the private key into the shell environment and make the key globally available to the user `root`:

```
sys1 # exec /usr/bin/ssh-agent $SHELL
sys1 # ssh-add

  Identity added: //.ssh/id_dsa
```

This shell-specific step is valid only while the shell is active. You must execute the procedure again if you close the shell during the session.

To verify that you can connect to a target system

1 On the source system (sys1), enter the following command:

   ```
   sys1 # ssh -l root sys2 uname -a
   ```

   where sys2 is the name of the target system.

2 The command should execute from the source system (sys1) to the target system (sys2) without the system requesting a passphrase or password.

3 Repeat this procedure for each target system.

Restarting the ssh session

After you complete this procedure, ssh can be restarted in any of the following scenarios:

- After a terminal session is closed
- After a new terminal session is opened
- After a system is restarted
- After too much time has elapsed, to refresh ssh

To restart ssh

1 On the source installation system (sys1), bring the private key into the shell environment.

   ```
   sys1 # exec /usr/bin/ssh-agent $SHELL
   ```

2 Make the key globally available for the user root

   ```
   sys1 # ssh-add
   ```

Enabling and disabling rsh for Solaris

The following section describes how to enable remote shell on Solaris system.

Symantec recommends configuring a secure shell environment for Symantec product installations.

See "Manually configuring passwordless ssh" on page 8.

See the operating system documentation for more information on configuring remote shell.

To enable rsh

1   To determine the current status of `rsh` and `rlogin`, type the following command:

    ```
    # inetadm | grep -i login
    ```

    If the service is enabled, the following line is displayed:

    ```
    enabled online svc:/network/login:rlogin
    ```

    If the service is not enabled, the following line is displayed:

    ```
    disabled disabled svc:/network/login:rlogin
    ```

2   To enable a disabled `rsh`/`rlogin` service, type the following command:

    ```
    # inetadm -e rlogin
    ```

3   To disable an enabled `rsh`/`rlogin` service, type the following command:

    ```
    # inetadm -d rlogin
    ```

4   Modify the `.rhosts` file. A separate `.rhosts` file is in the `$HOME` directory of each user. This file must be modified for each user who remotely accesses the system using rsh. Each line of the `.rhosts` file contains a fully qualified domain name or IP address for each remote system having access to the local system. For example, if the root user must remotely access `sys1` from `sys2`, you must add an entry for `sys2.`*`companyname`*`.com` in the `.rhosts` file on `sys1`.

    ```
    # echo "sys2.companyname.com" >> $HOME/.rhosts
    ```

5   After you complete an installation procedure, delete the `.rhosts` file from each user's `$HOME` directory to ensure security:

    ```
    # rm -f $HOME/.rhosts
    ```

Mounting a software disc

Symantec software is provided on a DVD format disc. If you have the media kit, then get the software disc from the media kit.

To mount the software disc

1   Log in as superuser.

2   Place the Symantec software disc containing your product into a DVD drive
    connected to your system.

3   If Solaris volume management software is running on your system, the software
    disc automatically mounts as `/cdrom/cdrom0`.

4   If Solaris volume management software is not available to mount the DVD,
    you must mount it manually. Insert the disc and enter the following command:

    ```
    # mount -F hsfs -o ro /dev/dsk/c0t6d0s2 /dvd_mount
    ```

    where `c0t6d0s2` is the default address for the disc drive.

5   Change to the appropriate directory and product subdirectory to view the product
    release notes and installation guides, or install the products.

Downloading the Symantec Storage Foundation and High Availability Solutions software

One method of obtaining the Symantec Storage Foundation and High Availability
Solutions software is to download it to your local system from the Symantec website.

For a Trialware download, perform the following. Contact your Symantec
representative for more information.

To download the trialware version of the software

1   Open the following link in your browser:

    http://www.symantec.com/index.jsp

2   In Products and Solutions section, click the **Trialware** link.

3   On the next page near the bottom of the page, click **Business Continuity**.

4   Under Cluster Server, click **Download**.

5   In the new window, click **Download Now**.

6   Review the terms and conditions, and click **I agree**.

7   You can use existing credentials to log in or create new credentials.

8   Find the product that you want to download and select it. Continue with the
    installation.

If you download a standalone Symantec product, the single product download files do not contain the product installer. Use the installation script for the specific product to install the product.

Note: Trialware is the full product version. The enabled licensing places the product in a demo or a trial state.

See "About the script-based installer" on page 15.

To download the software

1 Verify that you have enough space on your filesystem to store the downloaded software.

  The estimated space for download, gunzip, and tar extract is 2 GB for SPARC.

  If you plan to install the software on the same system, make sure that you also have enough space for the installed software.

2 To see the space available, you can use the `df` command with the name of the local file system where you intend to download the software.

  ```
  # /usr/bin/df -l filesystem
  ```

Caution: When you select a location to download files, do not select a directory that contains Symantec products from a previous release or maintenance pack. Make sure that different versions exist in different directories.

---

3 Download the software, specifying the file system with sufficient space for the file.

Installing and upgrading prerequisites

See your product Installation Guide for more information.

About the script-based installer

You can use the script-based installer to install Symantec products (version 6.1 and later) from a driver system that runs any supported platform to a target system that runs different supported platforms.

To install your Symantec product, use one of the following methods:

- The general product installer (`installer`). The general product installer script provides a menu that simplifies the selection of installation and configuration options. Use the general product installer if you want to install multiple products from a disc.

- Product-specific installation scripts (`install<productname>`). The product-specific installation scripts provide command-line interface options. Installing and configuring with the `install<productname>` script is identical to running the general product installer and specifying SFHA from the list of products to install. Use the product-specific installation scripts to install or configure individual products you download electronically. You can find these scripts at the root of the product media. These scripts are also installed with the product.

The production installation scripts lists all the SFHA Solutions product installation scripts. The list of product-specific installation scripts that you find on your system depends on the product that you install on your system.

Table 1-1   Product installation scripts

Symantec product name	Script name in the media	Script name after an installation
For all SFHA Solutions products	`installer`	N/A
Symantec ApplicationHA	`installapplicationha`	`installapplicationha<version>`
Symantec Cluster Server (VCS)	`installvcs`	`installvcs<version>`
Symantec Storage Foundation (SF)	`installsf`	`installsf<version>`
Symantec Storage Foundation and High Availability (SFHA)	`installsfha`	`installsfha<version>`
Symantec Storage Foundation Cluster File System High Availability (SFCFSHA)	`installsfcfsha`	`installsfcfsha<version>`
Symantec Storage Foundation for Oracle RAC (SF Oracle RAC)	`installsfrac`	`installsfrac<version>`

Table 1-1   Product installation scripts *(continued)*

Symantec product name	Script name in the media	Script name after an installation
Symantec Storage Foundation for Sybase ASE CE (SF Sybase CE)	`installsfsybasece`	`installsfsybasece<version>`
Symantec Dynamic Multi-pathing (DMP)	`installdmp`	`installdmp<version>`

When you install from the installation media, the script name does not include a product version.

When you configure the product after an installation, the installation scripts include the product version in the script name.

For example, for the 6.2 version:

```
# /opt/VRTS/install/install<productname>62 -configure
```

Note: The general product installer (`installer`) script does not include the product version.

At most points during the installation you can type the following characters for different actions:

- Use `b` (back) to return to a previous section of the installation procedure. The back feature of the installation scripts is context-sensitive, so it returns to the beginning of a grouped section of questions.

- Use `Ctrl+c` to stop and exit the program if an installation procedure hangs. After a short delay, the script exits.

- Use `q` to quit the installer.

- Use `?` to display help information.

- Use the Enter button to accept a default response.

About the web-based installer

Use the web-based installer interface to install Symantec products. The web-based installer can perform most of the tasks that the script-based installer performs.

You use the `webinstaller` script to start and stop the Veritas XPortal Server `xprtlwid` process. The `webinstaller` script can also be used to check the status of the XPortal Server.

When the `webinstaller` script starts the `xprtlwid` process, the script displays a URL. Use this URL to access the web-based installer from a web browser such as Internet Explorer or FireFox.

The web installer creates log files whenever the web installer operates. While the installation processes operate, the log files are located in a session-based directory under the `/var/tmp` directory. After the install process completes, the log files are located in the `/opt/VRTS/install/logs` directory. Symantec recommends that you keep these files for auditing, debugging, and future use.

The location of the Veritas XPortal Server configuration file is `/var/opt/webinstaller/xprtlwid.conf`.

Starting and stopping processes for the Symantec products

After the installation and configuration is complete, the Symantec product installer starts the processes that the installed products use. You can use the product installer to stop or start the processes, if required.

To stop the processes

◆ Use the `-stop` option to stop the product installation script.

For example, to stop the product's processes, enter the following command:

`./installer -stop`

or

`/opt/VRTS/install/install<productname><version> -stop`

Where `<productname>` is the product acronym name such as *sf*.

Where `<version>` is the specific release version.

See "About the script-based installer" on page 15.

To start the processes

◆ Use the `-start` option to start the product installation script.

For example, to start the product's processes, enter the following command:

./installer -start

or

/opt/VRTS/install/install<productname><*version*> -start

Where *<productname>* is the product acronym name such as *sf*.

Where *<version>* is the specific release version.

See "About the script-based installer" on page 15.

Restarting the installer after a failed connection

If an installation is killed because of a failed connection, you can restart the installer to resume the installation. The installer detects the existing installation. The installer prompts you whether you want to resume the installation. If you resume the installation, the installation proceeds from the point where the installation failed.

Installation program has improved failure handling

The product installer has improved ability to recover from failed installations, as follows:

■ A recovery file is created if an installation fails due to a failed network connection. This file enables the install program to resume from the point where the installation failed.

■ New options are available to start or stop the Veritas processes without requiring a full installation or configuration.